

REMARKS

Applicants reply to the Final Office Action dated August 6, 2007 within the shortened three month statutory period for reply. Claims 1-49 were pending in the application and the Examiner rejects claims 1-49. Applicants amend some of the currently pending claims and add new dependent claim 50. Support for the amendments and the added claim may be found in the originally-filed specification, claims, and figures. No new matter has been introduced by these amendments and this new claim. Applicants respectfully submit that the application is in condition for allowance and request reconsideration of the pending claims. Applicants have herewith filed a Request for Continued Examination

SECTION 103(a) REJECTIONS

The Examiner rejects claims 1-49 under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 6,728,379 issued to Ishibashi ("Ishibashi"). Applicants respectfully traverse these rejections.

In reviewing the pending application in light of Ishibashi, Applicants respectfully submit that Ishibashi does not disclose at least three specific aspects that are disclosed in Applicants' specification and claimed as part of Applicants' invention:

- (1) Applicants' content decryption key is generated in a device that uses the generated content decryption key to decrypt the encrypted content, so the content decryption key is not required to be transferred to the content decryption device (see, e.g., FIGS. 1, 3-7). In contrast, Ishibashi's content decryption key is generated in a device that does not use the generated content decryption key to decrypt the content, so the content decryption key must be transferred to the appropriate content decryption device (see, e.g, FIGS. 6, 8);
- (2) Applicants' content keys do not need to be encrypted or decrypted (nowhere in the application do Applicants mention encrypting the content keys, whereas other items are clearly encrypted and decrypted) because they are not transferred outside the content encryption/decryption device. In contrast, Ishibashi's content keys must be

encrypted and decrypted because they are transferred outside of the encryption and decryption devices (see, e.g., col. 3, lines 58-60 and FIGS. 6, 8); and

- (3) Applicants' time-varying keys used in mutual authentication are not transferred between the encryption and decryption devices (see, e.g., FIGS. 1, 3-7). In contrast, Ishibashi's "session keys" (to which the Examiner compares Applicant's time-varying keys) are transferred between the encryption and decryption devices (see, e.g., FIGS. 6, 8).

Applicants respectfully submit that these three aspects are significant because they affect the security of Applicants' and Ishibashi's systems. For example, each time an encryption or decryption key is transferred between devices in Ishibashi's system, there is a greater chance of a security breach. Thus, it is highly advantageous that Applicants' encryption, decryption, and time-varying keys are not required to be transmitted outside of the device in which they are generated. Further, Applicants' system is more efficient than Ishibashi's system because Applicants' keys are not required to be encrypted.

Applicants have amended many of claims 1-49 and added claim 50 to clarify the above-listed three aspects. Applicants have also amended some of the claims to comply with certain formal requirements or to clarify the claims. Applicants respectfully submit that all of the amendments find support in the originally-filed application and that these amendments put all the claims in condition for allowance.

Independent claim 1 recites, in part, that "the content decryption device includes . . . a first decryption section for decrypting the encrypted contents using the contents decryption key generated by the second contents key generation section, wherein the contents decryption key is not required to be encrypted or decrypted by the content decryption device." Applicants respectfully submit that Ishibashi does not disclose every element of independent claim 1 because Ishibashi requires, among other things, that "the content provider 10 encrypts, by a distribution encryption key, a content decryption key for decryption of an encrypted content data" (col. 3, lines 58-60), and "the information processor 100 reads a distribution decryption key Kdd from the memory 134 of the cryptography processor 130, sends it to the content key decryption section 131, and decrypts an encrypted content decryption key Kde(Kcd)" (col. 10, lines 27-32, emphasis added; see also FIG. 8). Ishibashi would not function as disclosed without

encrypting and decrypting content keys, and, in fact, all decryption devices disclosed in Ishibashi require the decryption of content decryption keys.

Moreover, independent claim 1 also recites, in part, “wherein the content encryption device includes . . . a first contents key generation section for generating the contents encryption key based on a second decryption limitation obtained by updating a first decryption limitation.” Applicants’ previous reply argued that Ishibashi does not disclose these elements of claim 1 because “neither item 14 nor item 131 of Ishibashi generates a contents key Kcd based on a copy control code” (5/24/07 Reply at page 15; emphasis in original). The Examiner responded in the Final Office Action at page 3, “Therefore, Kcd^{cx} is an item that is generated by device 130, which is a content decryption key, and is generated based on the copy control code.” However, device 130 is located in information processor 100, which is not a contents encryption device as required by claim 1; rather, information processor 100 is a key encryption device. Ishibashi only discloses a single contents encryption device—content provider 10—all the other devices (e.g., 100, 200) only encrypt keys, and not content (see, e.g., FIGS. 6, 8, 10; col. 5, lines 13-8). The only device in Ishibashi that the Examiner could point to that “generates the contents encryption key based on a second decryption limitation obtained by updating a first decryption limitation” is information processor 100—a key encryption device. Therefore, Ishibashi does not disclose a content encryption device that includes “a first contents key generation section for generating the contents encryption key based on a second decryption limitation obtained by updating a first decryption limitation.”

The Examiner argued that it would have been obvious to employ the functionality of device 130 in device 10 because “the content provider is interested in determining how many copies are to be made, and therefore there is a definite motivation to implement the copy control functionality at the server side” (Final Office Action at page 4). However, that motivation is inapposite because device 100 (where device 130 is located) is a completely different device than device 10, as discussed above, and claim 1 clearly requires a content encryption device. Ishibashi provides no support or motivation for employing the functionality of device 130 in anything but a key encryption device, but the Examiner seemed to argue that device 10 and device 130 were both key encryption devices. Therefore, at least for these reasons, Applicants respectfully submit that Ishibashi does not disclose or render obvious each element of claim 1.

Independent claim 26 recites, in part, “a contents key generation section within the decryption device for generating the contents decryption key from the second decryption limitation, wherein the contents decryption key is not required to be transferred to or from the encryption device and is not required to be encrypted or decrypted,” and independent claim 37 recites, in part, “wherein the contents key is not required to be transferred to or from the encryption device.” As discussed regarding similar limitations of independent claim 1, Ishibashi requires that the contents encryption and decryption keys be encrypted, transferred between encryption/decryption devices, and/or decrypted. Therefore, at least for this reason, Applicants respectfully submit that Ishibashi does not disclose or render obvious each element of claim 26.

Additionally, independent claim 14 recites, in part, “An encryption device . . . comprising . . . a second encryption section for encrypting the first decryption limitation using a time-varying key and outputting a second encrypted decryption limitation to the decryption device without transmitting the time-varying key to the decryption device.” Applicants do not disclose any encryption or decryption of the time-varying key, and the time-varying key is not transferred between the encryption and decryption devices (see, e.g, FIGS. 1, 3-7). Ishibashi, on the other hand, requires that the time-varying key be transferred between the encryption and decryption devices: “At step 2, the session key K_{session} is shared by both the key distribution center 30 and information processor 100” (col. 7, lines 41-43; see also FIGS. 6, 8), and “At step 2, the session key K_{session} is shared between the information processors 100 and 200” (col. 12, lines 51-53). The Examiner alleged in the Final Office Action that “[Applicants’] time varying key is represented by [Ishibashi’s] session key” (Final Office Action at page 5). Therefore, Applicants respectfully submit that for at least this reason Ishibashi does not disclose or render obvious each element of claim 14.

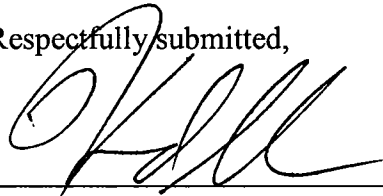
CONCLUSION

Therefore, because Ishibashi does not disclose or suggest at least the three elements listed above, as recited in amended independent claims 1, 14, 26 and 37, Applicants respectfully submit that all the independent claims are allowable over Ishibashi.

Dependent claims 2-13, 15-25, 27-36 and 38-50 variously depend from independent claims 1, 14, 26 and 37, so Applicants respectfully submit that dependent claims 2-13, 15-25, 27-36 and 38-50 are differentiated from the cited reference for the same reasons as set forth above, in addition to their own respective features.

In view of the above remarks, Applicants respectfully submit that all pending claims properly set forth that which Applicants regard as their invention and are allowable over the cited reference. Accordingly, Applicants respectfully request allowance of the pending claims. The Examiner is invited to telephone the undersigned at the Examiner's convenience if it would help further prosecution of the subject Application. The Commissioner is authorized to charge any fees due to Deposit Account No. 19-2814.

Respectfully submitted,



Howard I. Sobelman
Reg. No. 39,038

Dated: 10/29/07

SNELL & WILMER L.L.P.
400 E. Van Buren
One Arizona Center
Phoenix, Arizona 85004
Phone: 602-382-6228
Fax: 602-382-6070
Email: hsobelman@swlaw.com